aruba
a Hewlett Packard Enterprise company

Lucerne University of Applied Sciences and Arts
HOCHSCHULE LUZERN

Intelligent Edge Protection

Oliver Wehrli, Technology Consultant

#HSLU

Intelligent…what?

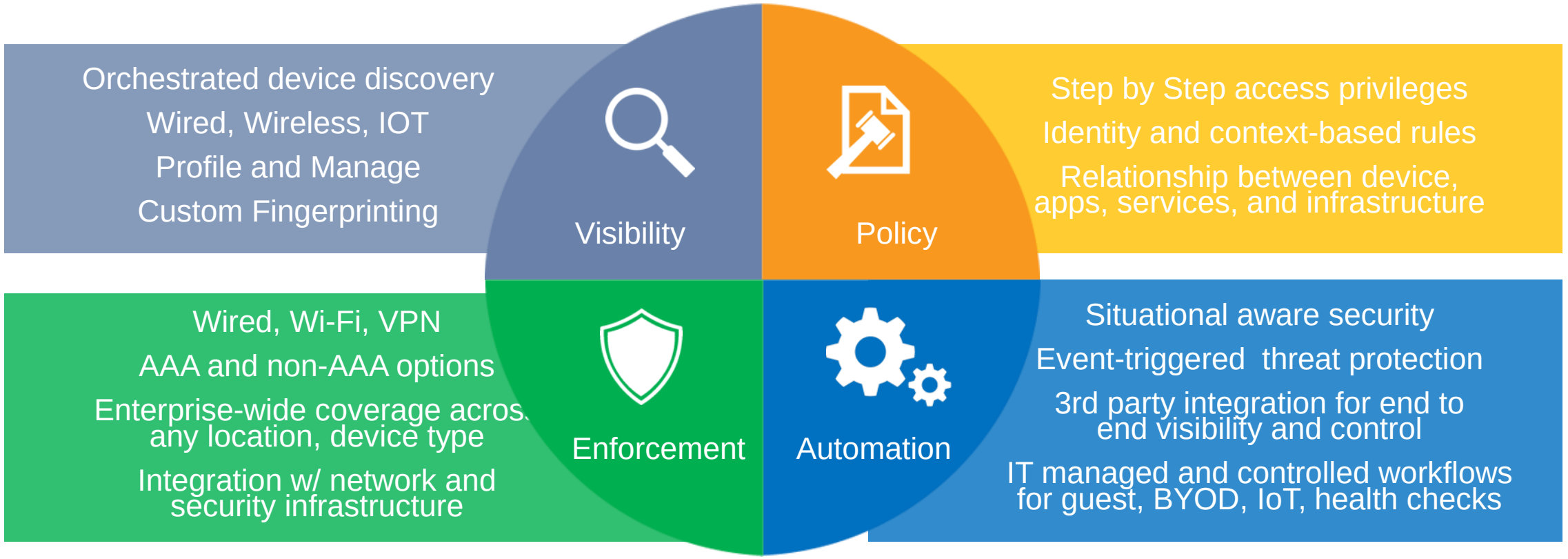
aruba
a Hewlett Packard Enterprise company

“Aruba takes untrusted devices and converts them into sources of trusted and actionable data”

The Fundamentals of Network Access

- **Profile** the Asset
  - Asset, location and basic posture information
  - Passive and active techniques
- **Validate** the Identity
  - Traditional network authentication methods 802.1x, MAC, PSKs
  - Leverage profile data as input to identity
  - Reference an existing asset register or start building one
- **Authorize** its Role
  - Lookup existing databases or trigger approval workflows
  - IT policies about security behavior, risk, access control
  - OT policies regarding SLA, auditing, compliance

The 4 stages of visibility and control



aruba
a Hewlett Packard Enterprise company

Sources of Usable Context

Device Profiling

- Samsung SM-G900
- Android
- “Jons-Galaxy”

EMM/MDM

- Personal owned
- Registered
- OS up-to-date

- Hansen, Jon [Sales]
- MDM enabled = true
- In-compliance = true

Identity Stores

- Hansen, Jon [Sales]
- Title – COO
- Dept – Executive office
- City – London

Active Directory

Office 365

MySQL

Google Apps

SAML

OAUTH 2

Enforcement Points

- Location – Bldg 10
- Floor – 3
- Bandwidth – 10Mbps

Comprehensive Profiler Methods

Helps ensure accurate fingerprints

Passive Profiling

- DHCP Fingerprinting (MAC OUI & Certain Options)
  - DHCP Relay or SPAN
- HTTP User-Agent
  - AOS IF-MAP Interface, Guest and Onboard Workflows
- TCP Fingerprinting (SYN, SYN/ACK)
  - SPAN
- ARP
  - SPAN
- Cisco Device Sensor
- Netflow/IPFIX
  - Identifies open ports

Active Profiling

- Windows Management Instrumentation (WMI)
- Nmap
- MDM/EMM
- SSH
- ARP Table
  - SNMP
- MAC/Interface Table
  - SNMP
- CDP/LLDP Table
  - SNMP





aruba
a Hewlett Packard Enterprise company

ClearPass Policy Manager

Automated workflows

Enhanced security for BYOD and guests

Rules by user role and device types

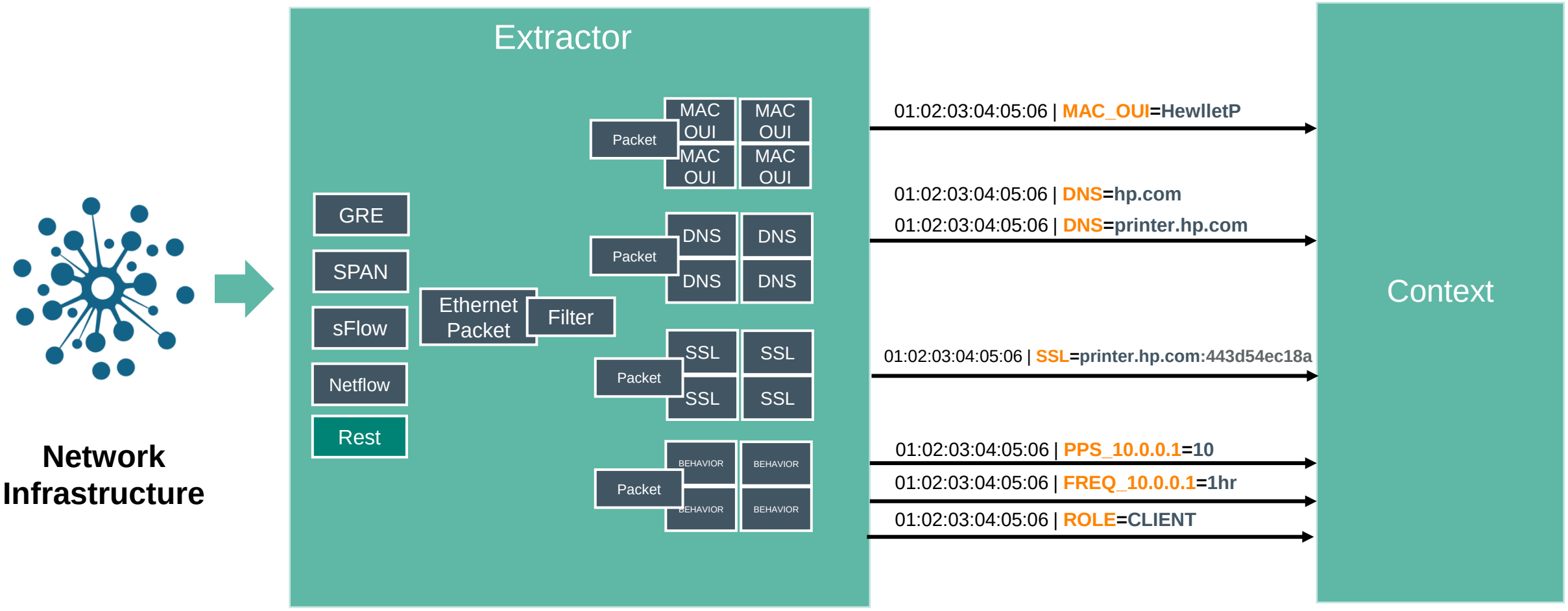
Onboard

Guest

OnGuard

aruba
a Hewlett Packard Enterprise company

From encapsulated packets to context

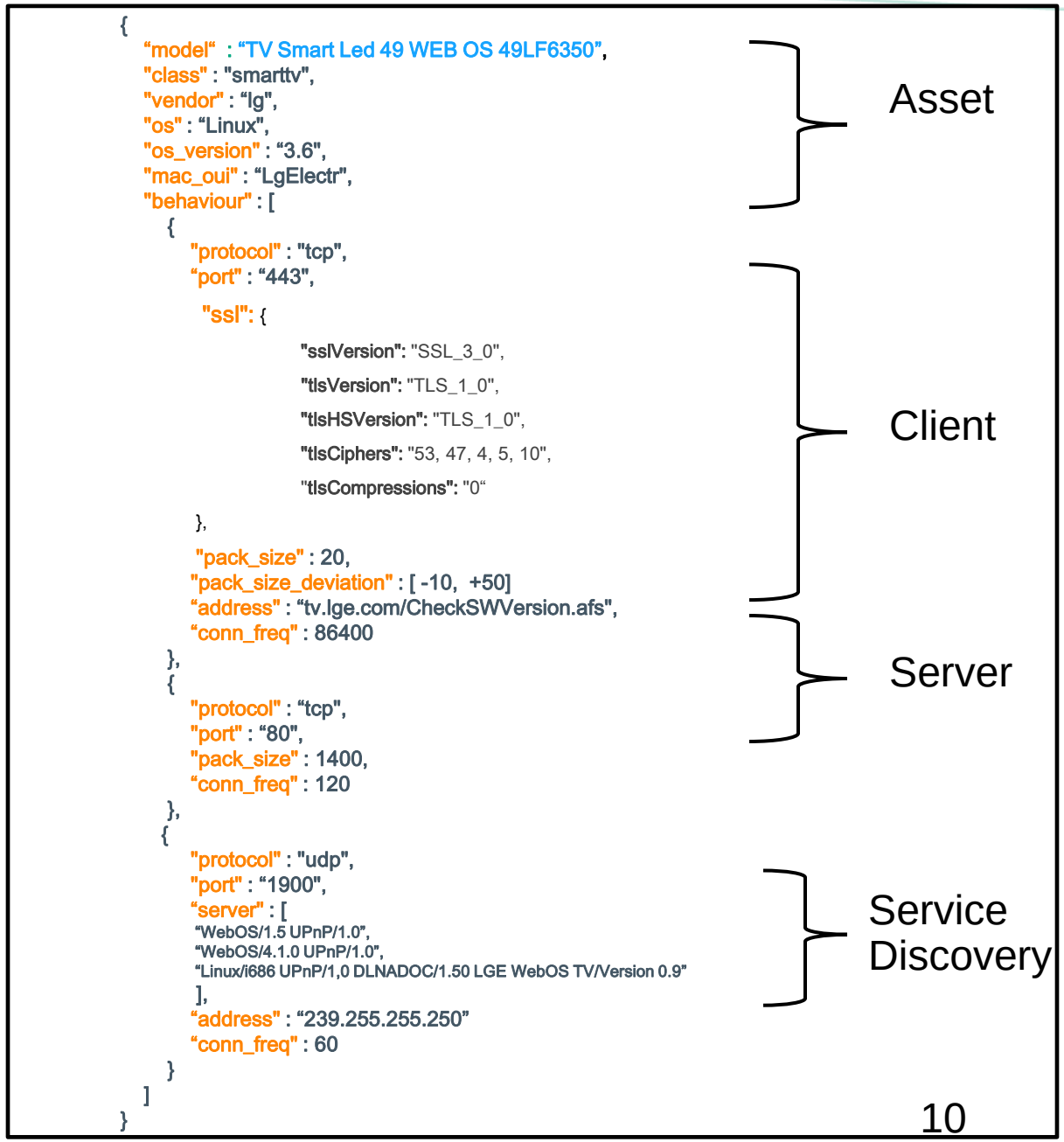


aruba
a Hewlett Packard Enterprise company

Modelling an Endpoint

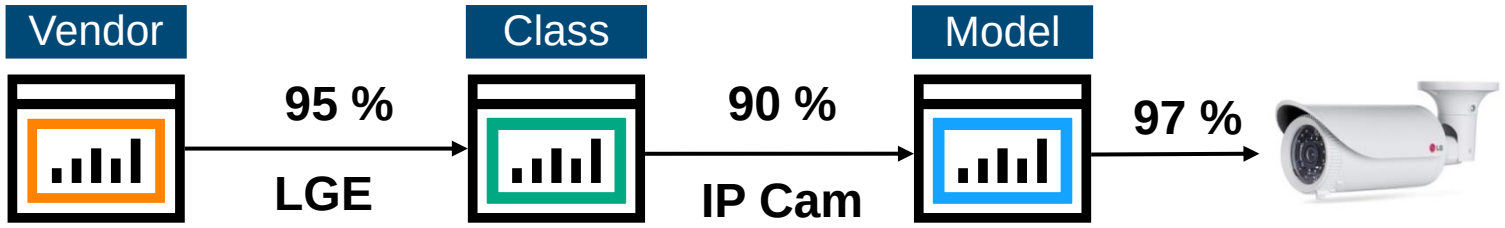
- Model dynamic behavior
  - Asset
  - Client
  - Server
  - Service discovery

- Example Parmeters
  - MAC_OUI, DHCP options
  - Operating System
  - Connections to a server using SSL on port 443
  - Used as HTTP Server on port 80
  - Uses SSDP on UDP port 1900 to annouce services every min



From context to classification

Weighted Bayesian Network



Training

Devices Database

MAC OUI	DHCP Vendor	Vendor
Hewlett-Packard	Hewlett-Packard JetDirect	HP
LgElectr	NA	LGE
LgElectr	LG Eletr	LGE
Sony	udhcp 1.15.3	Sony
Samsung	NA	Samsung
NOVELL	NA	Centrium

DHCP OPTS	Roles	TCP SYN	Class
1,3,10,35,20,50	Client	5FDAD1	IP Cam
1,3,10,35,20,50	Client Server	3235FD	IP Cam
2,5,6,9,15,60	Client	78DD69	smarttv
2,5,6,13,15,60	Client	DA4689	smarttv

Connection	SSL Ciphers	DHCP 55	Model
cam.lg.com:443	1,3,8,9,3	3,7,8,15,60	LNU3230R
:554		3,7,8,15,61	LNB5320
local:8080		3,7,8,15,62	LNU7210R

What if a new IP Cam model is released?

Extend the Device Schema

IT
Security Zone: **PCI Network**
Device Role: **Store Managed Devices**
Database Server: **10.4.20.120**
IP Address: **192.168.20.200**
CA Server: **10.4.20.200**
Managed Asset: **No**

OT
Serial Number: **313397773**
Asset Tab: **HJSYUHD2323**
SLA: **Category B**
Critical Dates: **Fridays 4pm**
Bandwidth Contract: **2Mb**
Store Location: **Pike Place, Seattle**
Installation Date: **July 10, 2016**

Asset Data
Vendor: **Traulsen**
Class: **Beverage Fridge**
Model: **4500Z**
Mac Address: **AA:BB:CC:11:22:33**
OS: **CentOS 7 (1511)**
Firmware Version: **12.17a**
Serial Number: **313397773**
NAS: **7010 Port 07**

Behavior
Connected Ports: **443**
Connected URLs: **supplier.com**
Risk Profile: **Low**
Polling Frequency: **Daily**
Bandwidth: **Normal**
Last Evaluation: **20161807-14:21:33**
Uptime: **34 Days**

Anomalies
New Ports: **25, 80**
New URLs: **competitor.com**
BW Deviation: 1**5%**
Polling Deviation: 2**5%**
Reboots Today: **5**
Spoofing: **MAC, OS Vendor**

Use Case: IoT Device Security Incident

Operator — WHO

Asset DB — WHAT, WHERE, WHEN

- Update switch (sandbox role, shutdown port)
- Update FW policy for store
- Block access to update URL
- Generate notifications to OT and IT
- Update risk profile for other fridges
- Flag inventory application to review data

Vendor: **Traulsen**
Class: **Beverage Fridge**
Role: **Store IoT devices**
Location: **Pike Place, Seattle**
Authentication: **MAC, SQL**
Mac Address: **AA:BB:CC:11:22:33**
Firmware Version: **12.35b**
Risk Profile: **High (open ports)**
Polling Frequency: **83 in last 5 mins**
BW Profile: **89% increase**

ClearPass Exchange

Granular traffic control with user and device data

Next-Gen Perimeter Defense

paloalto NETWORKS
Juniper NETWORKS ★
Check Point SOFTWARE TECHNOLOGIES LTD
FORTINET

Visibility and interactive control features

ArcSight An HP Company
splunk>
RSA SecurID
servicenow
QRadar
DUO ★

SIEM, Automation, MFA

Client Devices

IoT Devices

MDM / EMM

airwatch™
MobileIron
Google
CITRIX
Microsoft ★
BlackBerry

Network controls using real-time device data

aruba a Hewlett Packard Enterprise company
Hewlett Packard Enterprise
BROCADE
JUNIPER NETWORKS
CISCO

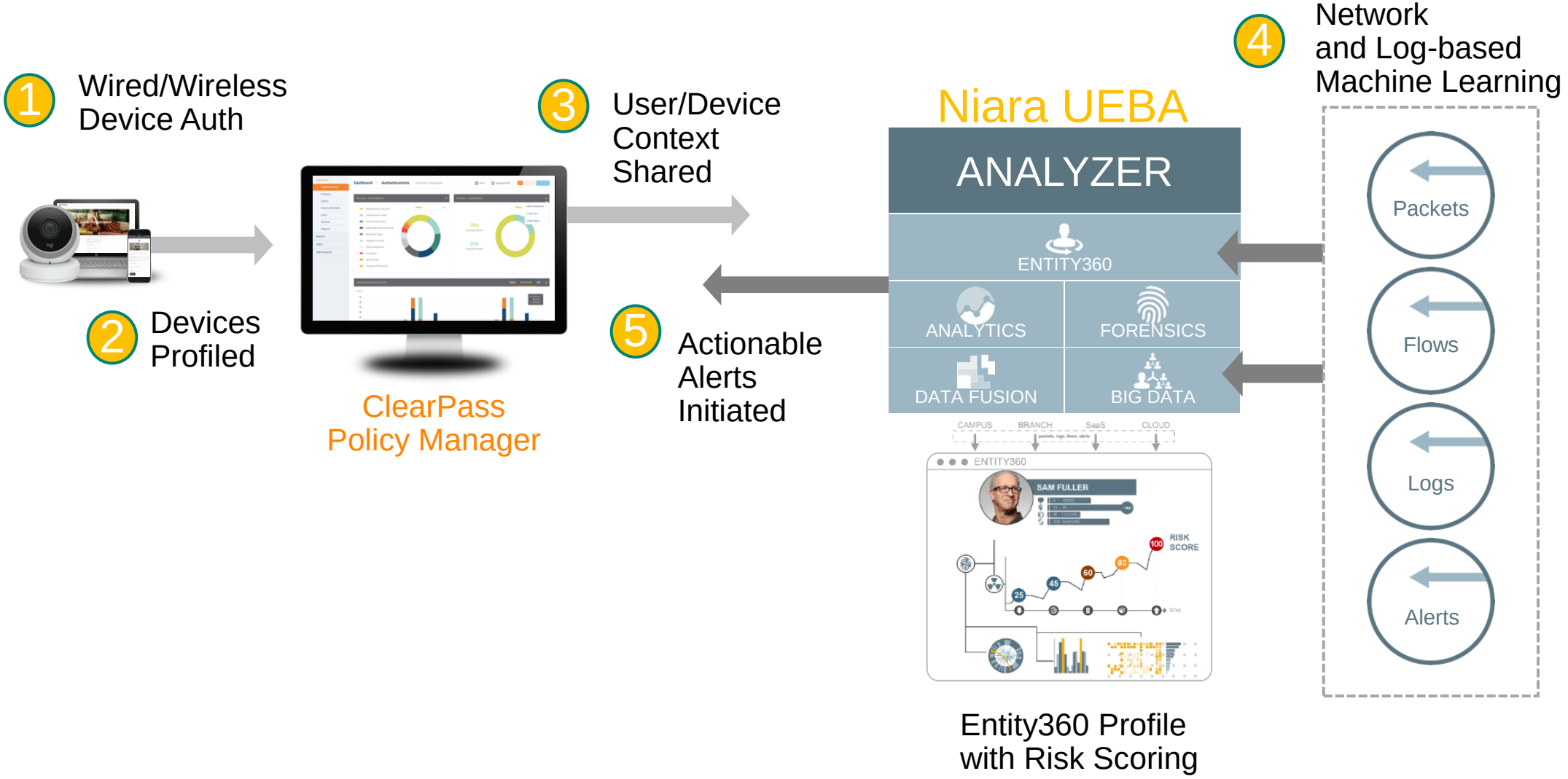
Infrastructure

Visibility into location and time with granular controls

aruba a Hewlett Packard Enterprise company

★ NEW

Automated Network and Security Controls



Entity360 Profile
with Risk Scoring

aruba
a Hewlett Packard
Enterprise company

Why all of this?

- BYOD, NAC, Guest Access, OT, IT
  - Different level of scale…..again
  - Cannot VLAN or MAC whitelist your way out of IoT
  - Automation a requirement, not a nice to have

- Role Based Access Control is key
  - Extend WLAN roles to the LAN and VPN
  - Leverage controllers for low bandwidth LAN devices
  - Firewall at the edge to help with network segmentation

OLIVER WEHRLI

TECHNOLOGY CONSULTANT | SWITZERLAND
T: +41 58 199 00 55

UEBERLANDSTRASSE 1 | CH-8600
DUEBENDORF | SWITZERLAND

AIRHEADS COMMUNITY | **FOLLOW US** | **Twitter** | **LinkedIn**

Thank You